

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
DOCKET NO: 3:18-CR-00311-MOC-DCK-3**

UNITED STATES OF AMERICA

vs.

MANUEL MAURO CHAVEZ,

Defendant.

)
)
)
)
)
)
)

ORDER

THIS MATTER is before the Court on Defendant’s Motion to Suppress evidence obtained from his social media account pursuant to an electronic search warrant. (Doc. No. 74). After an evidentiary hearing and several rounds of briefing, this matter is now ripe for review. For the reasons that follow, the Court denies Defendant’s Motion to Suppress.

I. BACKGROUND

A. Factual Background

In late 2009, law enforcement officers from several federal agencies began investigating a transnational fraudulent scheme. About nine years later, on June 25, 2018, the officers applied for a search warrant from United States Magistrate Judge Cayer. To support the application, United States Postal Investigator Mark Heath submitted an affidavit providing extensive details regarding the alleged scheme. The following facts are taken from that affidavit.

Essentially, the scheme unfolded as a fraudulent sweepstakes targeting United States residents, many of whom are elderly. Telemarketers in Costa Rica purportedly phoned their victims, then used various opening pitches to deceive them into believing they had won large monetary prizes in a sweepstakes. Of course, there was a catch: the victims had to wire transfer funds as an “insurance fee” to receive their “winnings.” When victims were willing to pay,

telemarketers called them repeatedly, asserting additional fees had to be paid in order to claim the prize. This continued until the victims were unwilling to pay. (Doc. No. 74-1 at 14).

In September 2016, investigators received a report from one of the victims of this scheme who stated that she had received a call in June 2015 informing her that she had won a \$4.5 million sweepstakes but that she needed to pay certain fees upfront to collect her prize. Over the next six months, she sent over \$220,000 to various individuals through money orders and direct deposits in a fruitless attempt to claim a prize. (Id.). Officers obtained records for the bank accounts where the victim made her direct deposits. From the records, officers learned that co-defendant Paul Stiep owned one of those accounts and that, from September 2014 to January 2016, that account had received about \$760,000 in suspicious deposits. During that time, Stiep had also wired about \$613,000 to Costa Rican recipients. (Id. at 14–15).

Inspector Heath and another inspector interviewed Stiep on August 16, 2017. During the interview, Stiep admitted he was involved in the scheme. First, he confessed that the deposits in his account derived from victims who were attempting to claim prizes. Next, he admitted he knew that telemarketers were making false statements to induce victims to part with their money. According to Stiep, his role was to take the received funds and forward them to others. In exchange, Stiep kept between ten and fifteen percent of the funds received. (Id. at 15).

Stiep indicated that he received instructions from two individuals in Costa Rica: co-defendant Roger Roger and Eugenio Castro. During the interview, Stiep allowed the inspectors to search his phone, including Facebook messages that he had exchanged with Roger. In the messages, Stiep and Roger discussed fraudulent deposits, Stiep's commission, and how to structure transfers to avoid scrutiny from the Internal Revenue Service. Roger also floated having Stiep fly to Costa Rica and work as one of his telemarketers. (Id. at 15–16).

Furthermore, during the interview, Stiep stated that he introduced his friend, Defendant Manuel Chavez, to Roger and Castro. Defendant was a Facebook Friend of both Stiep and Roger. (Id. at 18). According to Stiep, Defendant “knowingly moved sweepstakes related victim money at the direction of Roger and Castro and was paid a commission to do [so].” (Id. at 15). While reviewing Stiep’s Facebook messages, officers discovered that Stiep had complained to Roger that “Manny” received a fifteen percent commission for his wire transfers while Stiep received only ten percent. (Id. at 16–17). Based on this information, the IRS reviewed Defendant’s bank accounts and discovered about \$227,731.95 in fraudulent deposits. At least some of those deposits came from reporting victims—including the victim who reported being defrauded in September 2016. The IRS also traced about \$202,926 in wire transfers, which were sent to multiple recipients in Costa Rica, including Castro. (Id. at 18–19).

In the supporting affidavit, Postal Inspector Heath also discussed his experience investigating large-scale fraudulent telemarketing schemes. He averred that participants “routinely utilize electronic communications [like Facebook] to distribute lead lists, relay information about victims mailing and wires and to share specific instructions with co-conspirators on how to wire funds overseas.” (Id. at 21). Inspector Heath detailed Facebook’s various features and the data it collects. He declared each piece of data can “provide crucial evidence of the ‘who, what, why, when, where, and how’ of the criminal conduct under investigation” and “can indicate who has used or controlled the Facebook account.” (Id. at 25).

On June 25, 2018, the magistrate judge found that Inspector Heath’s affidavit afforded probable cause to search and seize several forms of evidence, and thus commanded Facebook to “disclose[]” the following information from Defendant’s account:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook

passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos; photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the account is or was a "fan" of;
- (j) All past and present lists of friends created by the account;
- (k) All records of Facebook searches performed by the account;
- (l) All information about the user's access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which

Facebook users have been blocked by the account; [and]

- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of activities taken.

(Id. at 4–5). The magistrate judge then authorized the Government to “seize[]” any disclosed information “that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1956(a)(2)(A) (international money laundering) involving [Defendant and his alleged co-conspirators] since January 1, 2011, through present.” (Id. at 6).

B. Procedural Background

In September 2018, Defendant and six co-conspirators were charged in a twenty-count indictment for participating in the fraudulent sweepstakes. (Doc. No. 3). Once Defendant was arrested on that indictment, he filed this motion, seeking suppression of all evidence obtained from his Facebook account pursuant to the June 2018 search warrant.

In August 2019, this Court held a hearing to receive pertinent evidence. There, Defendant submitted Facebook Business Records detailing the privacy restrictions he chose for various Facebook content before the warrant was issued. Facebook provides a “customizable set of privacy controls, so users can protect their information from getting to third-party individuals,” and “[s]hared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with a single person.” (Doc. No. 95-1 at 1).

For most of his content—including activities, identifying information, and wall posts—Defendant restricted access to those he had accepted as Facebook “Friends.” (Doc. No. 95-4). Other content forms—including Defendant’s Friends list and private messages—were only viewable by him. (Doc. Nos. 74-1 at 23, 95-4 at 2). A few other categories of information—including Defendant’s name and “reshares” of Defendant’s posts—were viewable by the “Public,”

(Doc. No. 95-4 at 4), meaning “[a]nyone can see [that] information,” (Doc. No. 95-2 at 4). Finally, Defendant “[b]locked” four users, (Doc. No. 95-4 at 5), so those users are unable to see even the posts he “share[d] with the public,” see Facebook Help Center, Blocking People, <https://www.facebook.com/help/290450221052800> (visited Sept. 25, 2019).

Defendant also testified as to why he selected those privacy settings. According to Defendant, there were some types of information that he did not “a member of the general public . . . who was not a Facebook Friend” to see. Defendant explained he has “[r]oughly three or four hundred” friends, “[m]ost” of whom he has “known from something,” even if they did not have a “consistent relationship.” Still, Defendant explained he does not “often” see many of the individuals he is Facebook Friends with.

Next, Inspector Heath testified regarding his motives when seeking the warrant. The inspector indicated that he sought such an expansive Facebook disclosure because there may be individuals who officers “weren’t aware of yet up to that point who [Defendant] recruited to be part of the scheme and help move money.” Relying on his training and experience, as well as the magistrate judge’s judgment, the inspector believed there was probable cause to execute the warrant. He also testified that he complied with all search limitations provided by the warrant.

II. DISCUSSION

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. The Amendment was crafted to “safeguard the privacy and security of individuals against arbitrary invasions by government officials.” Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018). It is the Framers’ “response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial area, which allowed British officers to rummage through homes in an unrestrained search for

evidence of criminal activity.” Riley v. California, 573 U.S. 373, 403 (2014).

Defendant contends the Amendment requires this Court to suppress the evidence seized from his Facebook account. First, he argues that his Fourth Amendment rights are implicated because he has a legitimate expectation of privacy in the content of his social media account that was designated “non-public” at the time of the search. (Doc. No. 101 at 3–4).¹ Next, he asserts those rights were infringed upon because the issued search warrant lacked probable cause and was overbroad. (Doc No. 74 at 7–13). Finally, he maintains the good-faith exception to the exclusionary rule should not apply because it was objectively unreasonable for officers to rely on the facially deficient warrant. (Id. at 12–14).

As explained below, the Court agrees that Defendant had a legitimate expectation of privacy in the non-public content on his social media account and thus a valid warrant was required to search such content. Although the Court finds the officers had probable cause to search such content, the issued warrant was nevertheless overbroad. Still, the warrant was not so overbroad as to render the officers’ reliance on it objectively unreasonable. Accordingly, Defendant’s Motion to Dismiss is denied.

A. Legitimate Expectation of Privacy

“Not all government actions are invasive enough to implicate the Fourth Amendment.” United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010). Instead, the “capacity to claim the protection of the Fourth Amendment depends upon whether the person who claims the protection

¹ Plaintiff does not contend that his Fourth Amendment rights were infringed on under a traditional “property-based understanding of the Fourth Amendment.” Flordia v. Jardines, 569 U.S. 1, 5 (2013). But see United States v. Irving, 347 F. Supp. 3d 615, 623 (D. Kan. 2018) (recognizing Facebook Terms of Service provide “that the user owns all of the content and information and can control how to share it” (emphasis added)).

has a legitimate expectation of privacy in the invaded place.” United States v. Castellanos, 716 F.3d 828, 833 (4th Cir. 2013) (citation and alterations omitted). “‘In order to demonstrate a legitimate expectation of privacy, [the defendant] must have a subjective expectation of privacy,’ and that subjective expectation of privacy must be ‘objectively reasonable; in other words, it must be an expectation that society is willing to recognize as reasonable.’” Id. at 832 (citations omitted). The “burden of showing a legitimate expectation of privacy in the area searched rests with the defendant.” Id. If the defendant meets that burden, then “official intrusion into that private sphere qualifies as a search and requires a warrant supported by probable cause.” Carpenter, 138 S. Ct. at 2213. For the reasons explained below, the Court finds that Defendant has a legitimate expectation of privacy in the Facebook content he designated as non-public.

First, when evaluating whether a defendant manifested a subjective expectation of privacy, courts consider whether the defendant intentionally “took steps to avoid” “allow[ing] the public at large to access” pertinent evidence. United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010); see Smith v. Maryland, 442 U.S. 735, 743 (1979) (inquiring whether defendant “demonstrated an expectation of privacy by his own conduct” (emphasis added)); Katz v. United States, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.” (emphasis added)); Castellanos, 716 F.3d at 834 (inquiring whether defendant took “precautions to exclude others”); see also Warshak, 631 F.3d at 284 (same); United States v. Rheault, 561 F.3d 55, 59 (1st Cir. 2009) (same); United States v. Ramapuram, 632 F.2d 1149, 1155 (4th Cir. 1980) (same).

In this case, Defendant’s Facebook Business Records and testimony reveal that he acted with the intent to exclude the public from accessing select content on his Facebook profile. Although Defendant allowed the public to access select content—such as his name—Defendant

restricted access to other forms of content by limiting access to himself, or to the Facebook Friends that he accepted. (Id.).² At the hearing, Defendant testified that he implemented such restrictions because there was some content that he did not want “a member of the general public . . . who was not a Facebook Friend” to see. Defendant’s actions to exclude the public from certain non-public content demonstrates that he maintained a subjective expectation of privacy in that content. See Irving, 347 F. Supp. 3d at 621 (finding a “line between public and private access” as evincing an expectation of privacy); United States v. Westley, No. 3:17-CR-171, 2018 WL 3448161, at *6 (D. Conn. July 17, 2018) (recognizing a user’s expectation of privacy “depends, inter alia, on the user’s privacy settings” (quoting United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012))); United States v. Khan, No. 15-CR-286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) (same), aff’d, 937 F.3d 1042 (7th Cir. 2019).³

Second, this Court must determine whether Defendant’s subjective expectation of privacy is reasonable. Although “no single rubric definitively resolves which expectations of privacy are entitled to protection,” courts have identified a couple “basic guideposts.” Carpenter, 138 S. Ct. at 2213–14. First, the Fourth Amendment secures the “‘privacies of life’ against ‘arbitrary power.’” Id. at 2214 (citation omitted). Second, the “central aim” of the Amendment is “to place obstacles in the way of a too permeating police surveillance.” Id. (citation omitted).

² That Defendant allowed the public to access some content on his Facebook account does not render all content unprotected by the Fourth Amendment. See Carpenter, 138 S. Ct. at 2217 (“A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” (alterations and internal quotation marks omitted)).

³ To the extent Defendant argues he had a reasonable expectation of privacy in his social media content designated as viewable by the broader public, the Court disagrees. See Katz, 389 U.S. at 351 (acknowledging that which “a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection”).

Generally, the reasonableness of a search is “informed by historical understandings ‘of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted.’” Id. (citation and alterations omitted). Still, because “technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes,” courts have rejected “mechanical interpretation[s]” of the Amendment to “assure preservation of that degree of privacy against government [encroachment] that existed when the Fourth Amendment was adopted.” Id. (alterations omitted) (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001)); accord Riley, 573 U.S. at 375 (broadening Fourth Amendment protections for cell phones after recognizing that they “differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee’s person”).

With these guideposts in mind, it is useful to begin by comparing social media to other, more-traditional forms of communication. See Warshak, 631 F.3d at 285. For over a century, courts have routinely held that the Fourth Amendment protects letters and sealed packages while those items are in transit. See United States v. Jacobsen, 466 U.S. 109, 114 (1984); Ex parte Jackson, 96 U.S. 727, 733 (1877). The sender has a reasonable expectation of privacy in such items because they took steps to keep the items “free from inspection” during transit. Jackson, 96 U.S. at 733. Accordingly, during transit, such items “can only be opened and examined under [a valid] warrant . . . , as is required when papers are subjected to search in one’s own household.” Id. “Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private.” Warshak, 631 F.3d at 285.

As technology evolved, courts have extended similar protections to phones. In Katz v. United States, the Government attached a listening device to the outside of a public phonebooth to intercept a defendant’s phone calls. See 389 U.S. at 348. Recognizing “the vital role that the

public telephone has come to play in private communication,” the Supreme Court held that one who occupies a phone booth, “shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.” Id. at 361. Again, the Court protected private communications that might be intercepted prior to reaching their ultimate destination. See Warshak, 631 F.3d at 285.

As with sealed packages and private phone calls, it is objectively reasonable for an individual to expect privacy in non-public content that is entrusted to a social media website as the intermediary of the ultimate recipient.⁴ A narrower reading would fail to recognize how “technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes.” Carpenter, 138 S. Ct. at 2214. Through Facebook and other social media sites, users instantaneously convey intimate, momentous, and sometimes weighty information to close friends and family members spanning the entire globe. Cf. Warshak, 631 F.3d at 284. For example, a user might create a non-public Facebook post revealing that he is suffering from terminal cancer. Another user might privately announce that she is in the early stages of pregnancy. And a third user might send a Facebook group message to close friends criticizing a political candidate in an upcoming election. Combined, these forms of information would create a “revealing montage of the user’s life.” Riley, 573 U.S. at 396. To read the Constitution as entirely failing to protect such private information “is to ignore the vital role that [social media] has come to play in private communication.” Katz, 389 U.S. at 352.

Invoking the third-party doctrine, the Government contends Defendant has no legitimate

⁴ To be sure, the ultimate recipient of such content may share it with law enforcement, as the Fourth Amendment does not “protect[] a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.” Hoffa v. United States, 385 U.S. 293, 302 (1966); see Meregildo, 883 F. Supp. 2d at 526. But here, the Government obtained the information from Facebook—the intermediary—not from the recipient.

expectation of privacy in any content posted to social media because he voluntarily conveyed that information to Facebook. This argument fails to recognize the limits of the doctrine. To be sure, “third-party information relating to the sending and routing of electronic communication does not receive Fourth Amendment protection.” United States v. Graham, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (citing United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)), overruled on other grounds by Carpenter, 138 S. Ct. at 2206. As a result, just as mailing addresses and dialed phone numbers are not protected, routing information such as a Facebook user’s IP address is not protected. See Graham, 824 F.3d at 433; see, e.g., United States v. Shah, No. 5:13-CR-328, 2015 WL 72118, at *10 (E.D.N.C. Jan. 6, 2015) (collecting cases). But the third-party doctrine does not extend to information that is “not directed to a business, but simply sent via the business.” In re U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (emphases added); see Graham, 824 F.3d at 432–33; Johnson v. Duxbury, Massachusetts, 931 F.3d 102, 108 (1st Cir. 2019) (same); Warshak, 631 F.3d at 288 (same); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008); see also Smith, 442 U.S. at 744 (holding defendant’s expectation of privacy was not reasonable where he “voluntarily conveyed” information to a company in “the ordinary course of business” (emphasis added)). Defendant’s non-public Facebook posts and messages were certainly not directed to Facebook. Rather, Facebook was the intermediary through which they were sent to their ultimate recipients. Accordingly, the third-party doctrine is inapplicable.

Finally, without precedent, the Government argues Defendant’s expectation of privacy is unreasonable because his non-public posts were shared with “hundreds” of Facebook Friends, many of “whom . . . he barely had a relationship” with. (Doc. No. 103 at 7). Essentially, this argument presumes that courts can evaluate Defendant’s interpersonal relationships and withhold Constitutional protections from those they deem insufficiently meaningful. The implications of

this presumption are startling. For example, a court could render private messages with an ex-spouse or estranged parent unprotected by finding those relationships insubstantial. Such a result would certainly be contrary to the Framers’ intentions to secure the privacies of life against arbitrary power. See Carpenter, 138 S. Ct. at 2213–14.

Fundamentally, this argument ignores that individuals—not the Government—are responsible for determining which relationships are worthwhile. Over a lifetime, humans form countless social bonds with varying degrees of intimacy. The very decision to confide personal information into another person can cultivate familiarity into friendship. The Fourth Amendment protects the rights of individuals to enter into such intimate relationships—without Government scrutiny of such relationships. See Lawrence v. Texas, 539 U.S. 558, 562 (2003) (recognizing that “[l]iberty protects the person from unwarranted government intrusions” and that “the State is not omnipresent”); see also Monu Bedi, Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply, 54 B.C. L. Rev. 1, 47 (2013); Thomas P. Crocker, From Privacy to Liberty: The Fourth Amendment After Lawrence, 57 UCLA L. Rev. 1, 26 (2009); James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1151 (2009).⁵

In sum, Defendant manifested a subjective expectation of privacy in his non-public Facebook content that society is prepared to recognize as reasonable. As such, Defendant’s legitimate expectation of privacy is protected by the Fourth Amendment.

B. Probable Cause

Because Defendant has a legitimate expectation of privacy in his non-public Facebook

⁵ Courts do consider whether the individual has a “right . . . to exclude others” from pertinent evidence. Castellanos, 716 F.3d at 834; see Rakas v. Illinois, 439 U.S. 128, 149 (1978). But recognizing that an individual has a right to exclude others is very different than assessing why an individual chose to confide in another person. As discussed above, it is for the individual, not for the Government, to decide which relationships deserve such confidence.

content, the Fourth Amendment commands officers to obtain a valid warrant before searching that content. See United States v. Lyles, 910 F.3d 787, 791 (4th Cir. 2018). Such warrants must be “issued by a neutral magistrate and supported by probable cause.” United States v. Montieth, 662 F.3d 660, 664 (4th Cir. 2011); see U.S. Const. amend. IV.

When determining whether a warrant is supported by probable cause, magistrates “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” United States v. Bosyk, 933 F.3d 319, 339 (4th Cir. 2019) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). This probable cause inquiry is “not a high bar.” Id. (quoting District of Columbia v. Wesby, 138 S. Ct. 577, 586 (2018)). “And officers need not ‘rule out a suspect’s innocent explanation for suspicious facts’ to obtain a warrant.” Id. (citation omitted).

Where a magistrate issued a challenged warrant, reviewing courts do not “assess probable cause de novo.” Id. Instead, we “limit our inquiry to whether there was a ‘substantial basis for determining the existence of probable cause.’” Montieth, 662 F.3d at 664 (quoting Gates, 462 U.S. at 239). In so inquiring, we “accord ‘great deference’ to the magistrate’s assessment of the facts presented to him.” Id. But we “may not go beyond the information actually presented to the magistrate during the warrant application process.” Lyles, 910 F.3d at 791.

Investigator Heath’s affidavit plainly provided the magistrate judge with a substantial basis to believe Defendant was involved in the fraudulent telemarketing scheme. The victim reports and fraudulent banking activity records provide cause to believe that such a fraudulent scheme was occurring. See United States v. Akinkoye, 185 F.3d 192, 199 (4th Cir. 1999). And Defendant was tied to that scheme through co-defendant Stiep’s self-incriminating confession and through his own fraudulent banking activity involving known victims. See United States v. Oloyede, 933 F.3d

302, 318 (4th Cir. 2019); United States v. Patterson, 150 F.3d 382, 386 (4th Cir. 1998) (reasoning that “an informant’s statement has an indicia of reliability when it is self-incriminating” and thus holding “a co-defendant’s confession that he and the suspect committed the crime, and used certain instrumentalities, supplies probable cause for arrest and seizure” (citation omitted)).

The affidavit likewise provides a substantial basis to believe Defendant’s particular Facebook account would contain evidence of the scheme. See United States v. Suarez, 906 F.2d 977, 984 (4th Cir. 1990) (recognizing there must be probable cause to search “a particular place”); United States v. Whitt, No. 1:17-CR-60, 2018 WL 447586, at *2 (S.D. Ohio Jan. 17, 2018) (requiring the Government to establish probable cause to “believe[] that relevant evidence may reside on the particular suspect’s Facebook account”). First, Inspector Heath averred that his experiences have taught him that fraudulent telemarketing schemes “routinely utilize electronic communications [like Facebook] to distribute lead lists, relay information about victims mailing and wires and to share specific instructions with co-conspirators on how to wire funds overseas.” (Doc. No. 74-1 at 21). A consent search of Stiep’s Facebook account revealed that he and Roger used Facebook’s messaging feature in this particular scheme to share such information. (Id. at 16–17). And Chavez, a potential third member of the fraudulent scheme, was Facebook Friends with both Stiep and Roger. (Id. at 18–19). Again, probable cause is not a high bar. See Bosyk, 933 F.3d at 339. And this Court’s inquiry is even more limited, inquiring only whether there is a substantial basis for determining the existence of probable cause. See Monteith, 662 F.3d at 664. At a minimum, these facts provide a substantial basis for finding probable cause to believe that Defendant’s Facebook account likewise might have been used to facilitate the fraudulent scheme.

Although there was probable cause to search Defendant’s Facebook account, this does not end the Court’s inquiry. Under the particularly requirement of the Fourth Amendment, a warrant

may “not be broader than the probable cause on which it is based.” United States v. Hurwitz, 459 F.3d 463, 472 (4th Cir. 2006). “The particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description leaves nothing to the discretion of the officers executing the warrant.” United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010). Defendant argues that the Facebook disclosure aspect of the warrant was so broad that it failed the particularity requirement of the Fourth Amendment. For the reasons discussed below, the Court agrees.

The warrant here is virtually identical to the described warrant in United States v. Blake, 868 F.3d 960, 966 (11th Cir. 2017), cert. denied sub nom. Moore v. United States, 138 S. Ct. 753 (2018), and cert. denied, 138 S. Ct. 1580 (2018). There, the Government successfully obtained two warrants, which “required Facebook to ‘disclose’ to the government virtually every type of data that could be located in a Facebook account.” Id. at 966. Such data included:

every private instant message [the defendant] had ever sent or received, every IP address she had ever logged in from, every photograph she had ever uploaded or been “tagged” in, every private or public group she had ever been a member of, every search on the website she had ever conducted, and every purchase she had ever made through “Facebook Marketplace,” as well as her entire contact list.

Id. The compelled disclosure was not limited to the period of time that the crime allegedly occurred. Id. Nor was the disclosure limited to evidence of the crime. Id. Indeed, the only limitation was that “after all the data had been ‘disclosed,’” law enforcement would only “seize[]” “data that ‘constitute[d] fruits, evidence, and instrumentalities’ of a specified crime.” Id. (second alteration in original).

After finding that other relevant warrants were “okay,” the Eleventh Circuit reasoned that “[t]he Facebook warrants are another matter.” Id. at 974. The Facebook warrants were troublesome because they “required disclosure to the government of virtually every kind of data

that could be found in a social media account. And unnecessarily so.” Id. For example, as to private Facebook messages, “the warrants could have been limited the request to messages sent to or from persons suspected at that time of being [involved in the criminal activities].” Id. And the warrants could have “requested data only from the period of time during which [the defendant] was suspected of taking part in the [criminal] conspiracy.” Id.

Similarly, in this case, Inspector Heath’s affidavit emphasizes that officers uncovered evidence “consistent with telemarketing fraud as early as January 2011.” (Doc. No. 74-1 at 15). Officers likewise identified potential members of the fraudulent scheme, including Defendant, Stiep, and Roger. (Id. at 12). Despite these discoveries, the Government compelled Facebook to disclose sixteen broad categories of evidence, without limiting disclosure to the purported members or purported dates. This compelled disclosure is “broader than the probable cause on which it is based.” Hurwitz, 459 F.3d at 472; see Blake at 974; United States v. Shipp, 392 F. Supp. 3d 300, 311 (E.D.N.Y. 2019); Irving, 347 F. Supp. 3d at 624 (recognizing that a search of “Defendant’s entire Facebook account” without being “defined and limited by the crime” is “akin to a general warrant”); Westley, 2018 WL 3448161, at *16 (recognizing that the “absence of a date restriction” on a Facebook disclosure warrant could render such a warrant overbroad); see also Suarez, 906 F.2d at 984 (recognizing probable cause must “be present at the time and place of the search” (emphasis added)).⁶

⁶ After Facebook’s broad disclosure, the magistrate judge then commanded the Government to limit its “seizure” to evidence involving the alleged fraud and the time period that that the fraud occurred. A recent Fourth Circuit decision may render this process unlawful. See United States v. Under Seal, No. 19-1730, at 25 (4th Cir. Nov. 1, 2019) (recognizing a magistrate judge erred by authorizing the Government to create a “Filter Team” that reviewed whether disclosed evidence may be seized because this process “assign[s] judicial functions to the executive branch”). But Defendant challenged the scope of the disclosure and not the Government’s disclosure review. (Doc. No. 74). Regardless, this recent decision does not change the Court’s good-faith analysis.

C. The Good-Faith Exception

Although the Fourth Amendment protects the right to be free from unreasonable searches and seizures, it is silent as to how that right should be enforced. See Davis v. United States, 564 U.S. 229, 231 (2011). Therefore, to safeguard its guarantees, the Supreme Court created the exclusionary rule, “a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation.” Id. The exclusionary rule does not apply in all cases. Rather, suppression is limited to those instances where suppression will result in “appreciable deterrence” of Fourth Amendment violations. Id. at 237 (quoting United States v. Janis, 428 U.S. 433, 454 (1976)).

Generally, the deterrence objective is not served by suppressing evidence obtained by an officer acting in good-faith reliance on a search warrant issued by a magistrate. See United States v. Leon, 468 U.S. 897, 920 (1984); United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011). Consequently, courts do not suppress the fruits of a search conducted pursuant to a warrant, even a subsequently invalidated warrant, unless an objectively reasonable officer would have known the search was illegal despite the magistrate’s authorization. See United States v. Bynum, 293 F.3d 192, 195 (4th Cir. 2002). To that end, courts have identified several circumstances where a reasonable officer would not rely on a warrant. Pertinent here, the reasonable officer does not rely on a warrant that is “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.” Leon, 468 U.S. at 923. Defendant argues the warrant here was “facially deficient” by “failing to sufficiently particularize the information sought.” (Doc. No. 74 at 14). The Court disagrees.

The exclusionary rule was created to deter unlawful police activity—not “innocent police conduct.” Davis, 564 U.S. at 240. Courts suppress evidence that is obtained in violation of binding

precedent because “[r]esponsible law enforcement officers will take care to learn ‘what is required of them . . . and will conform their conduct to these rules.’” Id. But applying the Fourth Amendment to social media accounts is a relatively unexplored area of law with nuances that have yet to be discovered. See Westley, 2018 WL 3448161, at *16–17. Courts should not punish law enforcement officers who are on the frontiers of new technology simply because “they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions.” United States v. Wellman, No. 1:08-CR-43, 2009 WL 37184, at *7 (S.D.W. Va. Jan. 7, 2009), aff’d, 663 F.3d 224 (4th Cir. 2011).

As discussed, the officers rightly had probable cause to believe that a fraudulent telemarketing scheme was occurring, that Defendant was involved in that scheme, and that Defendant’s Facebook account would contain evidence of that scheme. See supra Part II.B. And while this Court finds that the warrant here “violated the particularity requirement, whether [it] did is not an open and shut matter; it is a close enough question” that executing officers reasonably could have believed the warrant was valid. Blake, 868 F.3d at 975. Accordingly, because the officers acted in objective good-faith reliance on the issued warrant, the Court denies Defendant’s Motion to Suppress.

III. CONCLUSION

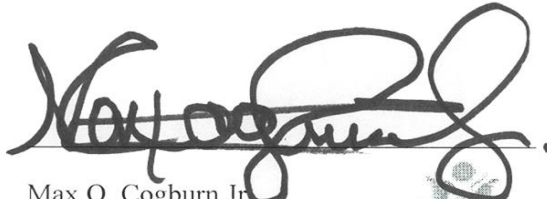
For the foregoing reasons, the Court finds that Defendant had a legitimate expectation of privacy in the non-public content on his Facebook account. Although officers had probable cause to search Defendant’s Facebook account for evidence of the fraudulent telemarketing scheme, the issued warrant was overbroad. Nevertheless, the warrant was not so facially deficient as to render reliance on it objectively unreasonable. Thus, the Court denies Defendant’s Motion to Suppress.

ORDER

IT IS, THEREFORE, ORDERED that Defendant's Motion to Suppress

(Doc. No. 74) is **DENIED**.

Signed: November 6, 2019



Max O. Cogburn Jr.
United States District Judge